

Welcome to the PIA for FY 2010!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: <http://www.privacy.va.gov/PIA.asp>

Roles and Responsibilities:

- Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.
- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.
 - b. Records Officer is responsible for supplying records retention and deletion schedules.
 - c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
 - d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
 - e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT customer, coordinating with the Privacy Officer and Information Security Officer and others who have concerns about privacy and security issues; and

systems, reviewing will the Privacy Officer, Information Security Officer, and units who have authority over security issues, and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

To enable macros, go to: 1) Tools > Macros - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

(FY 2010) PIA: System Identification

Program or System Name: LAN

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1180-00

Description of System / Application / Program: Local Area Network

Facility Name:	Atlanta, VA Medical Center		
Title:	Name:	Phone:	Email:
Privacy Officer:	Paula Marti	404-321-6111 x 2749	
Information Security Officer:	Felecia Beamon	404-321-6111 x5081	
Chief Information Officer:	Antonia Mohamed	404-321-6111 x6200	
Person Completing Document:	Felecia Beamon and Paula Marti		
Other Titles: LAB/NT Systems Manager	Allen Sandor	404-321-6111 x4634	
Other Titles:Network Manager	Jim Brougher	404-321-6111 x1578	
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	06/2008		
Date Approval To Operate Expires:	08/2011		
What specific legal authorities authorize this program or system:	Title 38, United States Code, Section 7301(a)		
What is the expected number of individuals that will have their PII stored in this system:	1,000-9,999,999		
Identify what stage the System / Application / Program is at:	Operations/Maintenance		

The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.

Is there an authorized change control process

which documents any changes to existing applications or systems?

If No, please explain:

Has a PIA been completed within the last three years?

Yes

Date of Report (MM/YYYY):

06/2008

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- Have any changes been made to the system since the last PIA?
- Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- Does this system/application/program collect, store or disseminate PII/PHI data?
- Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please skip to TAB 12. (See Comment for Definition of PII)

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):
79VA19
2. Name of the System of Records:
Vista-VA
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):
<http://yaww.vhaco.va.gov/privacy/SystemofRecords.htm>

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Does the System of Records Notice require modification or updating?

(Please Select Yes/No)

Is PII collected by paper methods?

Is PII collected by verbal methods?

Is PII collected by automated methods?

Is a Privacy notice provided?

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

Yes

Yes

Yes

Yes

Yes

Yes

Yes

(FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the Information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	All	Benefits/Healthcare/Research	Verbal & Written	All
Family Relation (spouse, children, parents, grandparents, etc)	All	Benefits/Healthcare/Research	Verbal & Written	All
Service Information	All	Benefits/Healthcare/Research	Verbal & Written	All
Medical Information	All	Benefits/Healthcare/Research	Verbal & Written	All
Criminal Record Information	All	Benefits/Healthcare/Research	Verbal & Written	All
Guardian Information	All	Benefits/Healthcare/Research	Verbal & Written	All
Education Information	All	Benefits/Healthcare/Research	Verbal & Written	All
Benefit Information	All	Benefits/Healthcare/Research	All	All
Other (Explain)	N/A			

Data Type	Is Data Type stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	verbally/On the form
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	verbally/On the form
Service Information	Yes	Veteran	Mandatory	verbally/On the form
Medical Information	Yes	Veteran	Mandatory	verbally/On the form
Criminal Record Information	Yes	Veteran	Mandatory	verbally/On the form
Guardian Information	Yes	Veteran	Voluntary	verbally/On the form
Education Information	Yes	Veteran	Voluntary	verbally/On the form

Benefit Information

	Veteran	Voluntary	Verbally/On the form
Yes	Yes	No	No
No	No	No	No
Other (Explain)			
Other (Explain)			
Other (Explain)			

(FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VA Health Eligibility Center	Yes	Patient information to assist with registration. Atlanta VA Regional Office has access to patient information to assist with adjudication of VA Beneficiary Claims	Both PII & PHI	These employees have their own Vista Accounts
Internal Sharing: VA Organization	VA Regional Office, Decatur	Yes	Name, Social Security Number, date of birth, and sex are transmitted to the Social Security Administration to track benefits.	Both PII & PHI	These employees have their own Vista Accounts
Other Federal Government Agency	Social Security Administration	No		PII	This is an electronic transfer.
Other Federal Government Agency	Internal Revenue Service	No	The SSN and first four characters of the surname are transmitted to Internal Revenue Service (IRS) in order to verify certain Veterans' self-reported income with federal tax information to identify Veterans' responsibility for making medical care copayments and enhance revenue from first party collections.	PII	This is an electronic transfer.
Other Federal Government Agency	Department of Defense	No	PHI and PII to facilitate a seamless transition for Veterans.	Both PII & PHI	This is an electronic transfer.
Local Government Agency					
Research Entity					

There is certain VHA Vista patient data that is shared with DoD through the Federal/Bidirectional Health Information Exchange (FHIE/BHIE) Program under DUAs that have been in effect for over three years. In addition, certain clinical information is being shared with CDC, also under an established DUA.

Other Project / System

Other Project / System

Both PII & PHI This is an electronic transfer.

Department of Defense

Other Project / System

(FY 2010) PIA: Access to Records

Does the system gather information from another system?
Please enter the name of the system:

No

Per responses in Tab 4, does the system gather information from an individual?

- No
 Through a Written Request
 Submitted In Person
 Online via Electronic Form

Is there a contingency plan in place to process information when the system is down?

Yes

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request?

Yes

- Research
 Sickle Cell
 Mental Health
 Other (Please Explain)

If yes, please check all that apply:

Describe process for authorizing access to this data.

There must be an
Authorization, Data Transfer
Agreement/ Usage
Agreement or
Memorandum of
Understanding authorizing
the secondary use.

Answer:

(FY 2010) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Data is collected electronically based on the automation of VA Forms and clinical procedures.

Individuals may either visit the VAMC where they receive their care and begin the process or may visit the Freedom of Information Act (FOIA) website at <http://www.gao.gov/ait/clo/foia/guide.sap#how> or may go through VA Forms at <http://www.va.gov/forms/medical/pdf/vha-10-5345-fill.pdf>. Further information regard the VA SOR is available at http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SPR_compilation.pdf.

Answer:

How is data checked for completeness?

Answer:

Data is reviewed by staff, compared to paper forms and verified with Next of Kin. Internal Audits are conducted on data for completeness and timeliness.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer:

How is new data verified for relevance, authenticity and accuracy?

Answer:

Clinical data is not removed. Administrative data is updated with each application for care.

New data is compared with printed form or via patient verification.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2010) PIA: Retention & Disposal

What is the data retention period?

Answer:

Explain why the information is needed for the indicated retention period?

Answer:

Clinical Information is retained in accordance with VA Records Control Schedule 10-1.

Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1.

What are the procedures for eliminating data at the end of the retention period?

Answer:

Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b. (Page 190). At the present time, Vista Imaging retains all Images. We are performing a study to explore whether some Images can be eliminated on an earlier schedule.

Where are these procedures documented?

Answer:

VA Handbook 6300; Record Control Schedule 10-1

How are data retention procedures enforced?

Answer:

VA Records Control Schedule 10-1 (page 8); Records Management Responsibilities The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. Field records officers are responsible for records management activities at their facilities. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Answer:

Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

No
Will information be collected through the Internet from children under age 13?
If Yes, How will parental or guardian approval be obtained?
Answer:

N/A

—

(FY 2010) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.

Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..

Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access?

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer:

At the department level the U.S. Office of Information Protection and Risk Management (OIPRM) is responsible for the establishment of directives, policies, & procedures which are consistent with the

1. Maintenance and preventative maintenance
2. Application Controls.
3. Construction/Environmental factors.
4. Data Integrity/Acces methodology.
5. Security awareness education and training for all employees

Explain what security risks were identified in the security assessment? (Check all that apply)

- Air Conditioning Failure
 Chemical/Biochemical Contamination
 Blackmail
 Bomb Threats
 Cold/Frost/Snow
 Communications Loss
 Computer Intrusion
 Data Destruction
 Data Disclosure
 Data Integrity Loss
 Denial of Service Attacks
 Earthquakes
 Eavesdropping/Interception
 Fire (False Alarm, Major, and Minor)
 Flooding/Water Damage
 Hardware Failure
 Malicious Code
 Computer Misuse
 Power Loss
 Sabotage/Terrorism
 Seisms/Hurricanes
 Substance Abuse
 Theft of Assets
 Theft of Data
 Vandalism/Rioting
 Errors (Configuration and Data Entry)
 Burglary/Break In/Robbery
 Identity Theft
 Fraud/Embezzlement

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. (Check off that apply)

- Risk Management
 Access Control
 Awareness and Training
 Continuity Planning
 Physical and Environmental Protection
 Personnel Security
 Certification and Accreditation Security Assessments

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.
Answer:

No additional choices were made as a result of performing this PIA

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?
(Choose One)

The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.

The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?
(Choose One)

The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.

The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization?
(Choose One)

The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.

The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments? The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; configuration, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response, maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility enjoys all security controls in the respects a high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

(FY 2010) PIA: VBA Minor Applications

Explain what minor application that are associated with your installation? (Check all that apply)

Records Locator System	Education Training Website	Appraisal System
Veterans Assistance Discharge System (VADS)	VR&E Training Website	Web Electronic Lender Identification
LGY Processing	VA Reserve Educational Assistance Program	CONDO PUD Builder
Loan Service and Claims	Web Automated Verification of Enrollment	Centralized Property Tracking System
LGY Home Loans	Right Now Web	Electronic Appraisal System
Search Participant Profile (SPP)	VA Online Certification of Enrollment (VA-ONCE)	Web LGY
Control of Veterans Records (COVERS)	Automated Folder Processing System (AFPS)	Access Manager
SHARE	Personal Computer Generated Letters (PCGL)	SAHSHA
Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	VBA Data Warehouse
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (blackberry)
Awards	State Benefits Reference System	VBA Enterprise Messaging System
Financial and Accounting System (FAS)	Training and Performance Support System (TPSS)	LGY Centralized Fax System
Eligibility Verification Report (EVR)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)
Automated Medical Information System (AMIS)290	Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Compensation and Pension (C&P)	Purchase Order Management System (POMS)
Web Service Medical Records (WebSMR)	Record Interchange (CAPRI)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)	Control of Veterans Records (COVERS)	Inventory Management System (IMS)
Fiduciary STAR Case Review	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Synquest
Veterans Exam Request Info System (VERIS)	Fiduciary Beneficiary System (FBS)	RAI/MDS
Web Automated Folder Processing System (WAFPS)	Hearing Officer Letters and Reports System (HOLAR)	Inforce
Courseware Delivery System (CDS)	Awards	ASSISTS
Electronic Performance Support System (EPSS)	Actuarial	MUSE
Veterans Service Representative (VSR) Advisor	Insurance Self Service	Bbraun (CP Memo)
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	VIC
C&P Training Website	Insurance Online	BCMA Contingency Machines
		Script Pro

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

	Name	Description	Comments
	Is PII collected by this min or application?		
Minor app #1		Does this minor application store PII? If yes, where?	
	Who has access to this data?		
	Name	Description	Comments
	Is PII collected by this min or application?		
Minor app #2		Does this minor application store PII? If yes, where?	
	Who has access to this data?		
	Name	Description	Comments
	Is PII collected by this min or application?		
Minor app #3		Does this minor application store PII? If yes, where?	
	Who has access to this data?		

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET) Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Priv Plus	BIRLS
Mental Health Assistant	Centralized Accounts Receivable System (CARS)
Telecare Record Manager	
Omnicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill	INS - BIRLS
Vocational Rehabilitation & Employment (VR&E) CH 31	Mobilization
Post Vietnam Era educational Program (VEAP) CH 32	Master Veterans Record (MVR)
Spinal Bifida Program Ch 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitlement Program for Survivors (REAPS)	
Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607	
Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS	
Work Study Management System (WSMS)	
Benefits Delivery Network (BDN)	
Personnel and Accounting Integrated Data and Fee Basis (PAID)	
Personnel Information Exchange System (PIES)	
Rating Board Automation 2000 (RBA2000)	
SHARE	
Service Member Records Tracking System	

(FY 2010) PIA: VISTA Minor Applications

Explain what minor application that are associated with your Installation? *(Check all that apply)*

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN) ADVERSE REACTION TRACKING ASISTS	DSS EXTRACTS EDUCATION TRACKING EOO COMPLAINT TRACKING	INTAKE/OUTPUT INTEGRATED BILLING INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT SUPPORT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	KERNEL
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KIDS
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	LAB SERVICE
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LETTERMAN
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LEXICON UTILITY
BED CONTROL	EXTENSIBLE EDITOR	LIBRARY
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIST MANAGER
CAPACITY MANAGEMENT - RUM	FEES BASIS	MAILMAN
CAPRI	FUNCTIONAL INDEPENDENCE	MASTER PATIENT INDEX VISTA
CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE
CARE MANAGEMENT CLINICAL CASE REGISTRIES	GEN. MED. REC. - I/O GEN. MED. REC. - VITALS	MEDICINE MENTAL HEALTH
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHVET
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original) A4EL
CMOP	HEALTH SUMMARY	NATIONAL DRUG FILE
CONSULT/REQUEST TRACKING	HINQ	NATIONAL LABORATORY TEST
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NDBI
CPT/HCPCS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NETWORK HEALTH EXCHANGE
CREDENTIALS TRACKING DENTAL DIETETICS	IFCAP IMAGING INCIDENT REPORTING	NOIS NURSING SERVICE OCCURRENCE SCREEN
DISCHARGE SUMMARY	INCOME VERIFICATION MATCH	ONCOLOGY
DRG GROUPER	INCOMPLETE RECORDS TRACKING	ORDER ENTRY/RESULTS REPORTING

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name	Description	Comments
Is PII collected by this min or application?		
Minor app #1	Does this minor application store PII? If yes, where?	
Who has access to this data?		

Name	Description	Comments
Is PII collected by this min or application?		
Minor app #2	Does this minor application store PII? If yes, where?	
Who has access to this data?		

Name	Description	Comments
Is PII collected by this min or application?		
Minor app #3	Does this minor application store PII? If yes, where?	
Who has access to this data?		

OUTPATIENT PHARMACY	SOCIAL WORK
PAID PATCH MODULE PATIENT DATA EXCHANGE	SPINAL CORD DYSFUNCTION SURGERY SURVEY GENERATOR
PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	TOOLKIT
PCE PATIENT CARE ENCOUNTER PCE PATIENT/IHS SUBSET	UNWINDER UTILIZATION MANAGEMENT ROLLUP
PHARMACY BENEFITS MANAGEMENT PHARMACY DATA MANAGEMENT PHARMACY NATIONAL DATABASE PHARMACY PRESCRIPTION PRACTICE POLICE & SECURITY	UTILIZATION REVIEW VA CERTIFIED COMPONENTS - DSSI VA FILEMAN VBECs VDEF
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS QUALITY ASSURANCE INTEGRATION QUALITY IMPROVEMENT CHECKLIST QUASAR	VISIT TRACKING VISTALINK VISTALINK SECURITY VISUAL IMPAIRMENT SERVICE TEAM ANRV
RADIOLOGY/NUCLEAR MEDICINE RECORD TRACKING	VOLUNTARY TIMEKEEPING VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI	CARE TRACKER
REMOTE ORDER/ENTRY SYSTEM RPC BROKER	
RUN TIME LIBRARY SAGG SCHEDULING	
SECURITY SUITE UTILITY PACK	
SHIFT CHANGE HANDOFF TOOL	

(FY 2010) PIA: Minor Applications

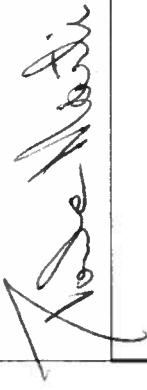
Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy these below sections as many times as needed.

	Name	Description	Comments
	Is PII collected by this min or application?		
Minor app #1	<input type="checkbox"/> Does this minor application store PII? <input type="checkbox"/> If yes, where?		
	<input type="checkbox"/> Who has access to this data?		
	Name	Description	Comments
	Is PII collected by this min or application?		
Minor app #2	<input type="checkbox"/> Does this minor application store PII? <input type="checkbox"/> If yes, where?		
	<input type="checkbox"/> Who has access to this data?		
	Name	Description	Comments
	Is PII collected by this min or application?		
Minor app #3	<input type="checkbox"/> Does this minor application store PII? <input type="checkbox"/> If yes, where?		
	<input type="checkbox"/> Who has access to this data?		

(FY 2010) PIA: Final Signatures

Facility Name: Atlanta, VA Medical Center

Title:	Name:	Phone:	Email:

Privacy Officer:	Paula Marti	404-321-6111 x 2749	0
 Digital Signature Block			

Information Security Officer:	Felecia Beamon	404-321-6111 x5081	0
Digitally signed by: FELECIA BEAMON DN: CN = FELECIA BEAMON O = Dept. of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.04.14 13:47:09 -05'00' Reason: I am the author of this document			

Chief Information Officer:	Antonia Mohamed	404-321-6111 x6200	0
 Digital Signature Block			

Person Completing Document:	Felecia Beamon and Paula Marti		
 Digital Signature Block			

System / Application / Program Manager:	Allen Sandor	#REF!	
 Digital Signature Block			

Date of Report:	4/8/2010		
OMB Unique Project Identifier	029-00-0111-01-1180-00		

Project Name

LAN